

FILED

US DISTRICT COURT

WESTERN DISTRICT
OF ARKANSAS

Nov 20, 2019

OFFICE OF THE CLERK

UNITED STATES DISTRICT COURT

for the
Western District of Arkansas
Fayetteville DivisionIn the Matter of the Search of
Samsung Galaxy S7 bearing
Identification number R58H817K83PCase No. 5:19 cm 126

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe property to be searched and give its location*): **See Attachment A**

located in the Western District of Arkansas, there is now concealed (*identify the person or describe the property to be seized*):
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. § 2251
 18 U.S.C. § 2252/2252A

Production of Child Pornography
 Possession/Distribution of Child Pornography

The application is based on these facts:

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



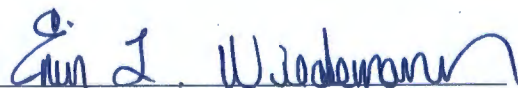
Applicant's signature

William DeVito, HSI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 11/20/19



Judge's signature

City and state: Fayetteville, Arkansas

Erin L. Wiedemann, Chief United States Magistrate Judge

Printed name and title

ATTACHMENT A
DESCRIPTION OF PROPERTY TO BE SEARCHED

Samsung Galaxy S7 bearing identification number R58H817K83P seized from Aaron GATEWOOD on September 24, 2019

ATTACHMENT B
ITEMS TO BE SEARCHED FOR AND SEIZED

- a. Any and all images of suspected child pornography and files containing images of suspected child pornography, any and all images believed to be an attempt to produce child pornography, in any form wherever it may be stored or found including, but not limited to:
 - i. originals, thumbnails, and copies of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
 - ii. videos (AKA motion pictures, films, film negatives), and other recordings or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
 - iii. Images self-produced of the defendant and minors, and attempts to take or produce such.
 - iv. Images of children, nude or otherwise, possessed, sent, received, or via message, email, or otherwise stored on the phone.
 - v. Internet history, including CACHE memory related to internet searches for child pornography or websites that could pertain such.
- b. information or correspondence pertaining to the solicitation of others for sexual activity involving minors, and any and all information, messages, etc related to the sexual exploitation of children, including but not limited to:
 - i. correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, text messages, establishing possession, identity of individuals, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
 - ii. records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
 - iii. Any and all address lists, names, contact information of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; and/or any information evidencing contact or correspondence with minors or adults in whatever form.

- iv. Any and all chat log, text messages, email, or any type of communication in any form, that is related to the sexual exploitation of minors for sexual purposes or related to the production, distribution or possession of child pornography.
- c. records evidencing ownership of the subject item, including in and all lists of names, telephone numbers, addresses and contacts, and the content of voice mails and text messages and internet-based applications, and internet or purchase history for any and all sexual devices, including but not limited to dildos, vibrators and sexual games.
- d. Any and all security devices, to include encryption devices, needed to gain access to the phone;
- e. Any and all address lists, names, contact information of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; and/or any information evidencing contact or correspondence with minors or adults in whatever form.
- f. Any and all recordings, including those made by the defendant or the minor victim, or anyone else that depicts the defendant or others engaging in sexually explicit conduct of any type.
- g. In searching the data, the computer personnel may examine and copy all of the data contained in the subject item to view their precise contents and determine whether the data falls within the items to be seized. In addition, the examining personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized.

ATTACHMENT C

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF ARKANSAS

STATE OF ARKANSAS

:
:
:
:

ss. AFFIDAVIT

COUNTY OF WASHINGTON

Affidavit in Support of Application for Search Warrant

I, William DeVito, being duly sworn, depose and state as follows:

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations (HSI), currently assigned to the Assistant Special Agent in Charge Office in Fayetteville, Arkansas. I have been so employed with HSI since July 2011. As part of my daily duties as an HSI Special Agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, online enticement, transportation, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2251A, 2422(b), 2252(a) and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also participated in the execution of numerous search warrants and arrest warrants, a number of which involved child exploitation and/or child pornography offenses. This affidavit is being submitted based on information from my own investigative efforts as well as information obtained from others who have investigated this matter and/or have personal knowledge of the facts herein.

2. This Affidavit is being submitted in support of an application for a search warrant

for electronic devices described as being a Samsung Galaxy S7 bearing identification number R58H817K83P, also referred to as "SUBJECT ITEM", located and seized from Aaron GATEWOOD's person at the time of his encounter and state arrest in Fayetteville, Arkansas, now being stored in evidence at the Homeland Security Office in Fayetteville, Arkansas. As such, it does not include all of the information known to me as part of this investigation, but only information sufficient to establish probable cause for the requested search warrant.

Statutory Authority

3. This investigation concerns alleged violations of Title 18, United States Code, Sections 2251, 2252 and 2252A, relating to material involving the sexual exploitation of minors, which has been defined in Title 18 U.S.C. 2256, as an individual under 18 years of age.

4. Under 18 U.S.C. Section 2251, it is a federal crime for any person using any means or facility of interstate and foreign commerce, to entice, use, persuade...a person that has not obtained the age of 18 years to engage in sexually explicit conduct for the purpose of creating a visual depiction of such conduct.

5. Under 18 U.S.C. Section 2252(a)(1) (transportation), 2252(a)(2) (receipt and distribution), and 2252(a)(4)(B) and 2252A(a)(5)(B) (possession), it is a federal crime for any person to transport, distribute, receive, and possess child pornography, as that term is defined by federal law. Further under 18 U.S.C. Section 2253(a)(3), a person who is convicted of an offense under 18 U.S.C. Section 2252 or 2252A, shall forfeit to the United States such person's interest in any property, real or personal, used or intended to be used to commit or to promote the commission of such offense.

**BACKGROUND REGARDING COMPUTER/ELECTRONIC DEVICES
AND THE INTERNET**

6. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

- a. Cell phones and more advanced devices known as “smart phones” function the same as computers and can run computer software and applications, create and edit files, access the Internet, chat, text, email, and interact with others on the Internet, and store, send, and receive files, among other functions. Cell phones and smart phones have been used by child pornographers to send, receive, store, and produce images depicting child pornography, as well as engage in voice, email, text, and real time chat conversations with minors and others. Cell phones and smart phones can contain SD cards and/or SIM cards that can store data such as pictures, videos, text messages, contact lists, call logs and other data.
- b. Computer technology, including mobile smart or cell phones, and the Internet have revolutionized the manner in which persons who have a sexual interest in children can communicate. The Internet affords individuals several different venues for meeting each other, meeting children and their parents, obtaining, viewing and trading child pornography in a relatively secure, and anonymous fashion.
- c. Computers including cell phones basically serve five functions in connection with child exploitation: production of child pornography, communication, distribution, storage, and social networking. In addition, new technologies are developing allowing average computer users avenues to mask their IP addresses for more private Internet browsing sessions.

- d. Through the Internet, electronic contact can be made to literally millions of computers around the world using any of their devices.
- e. As with most digital technology, communications made from a computer or smart phone are often saved or stored on that device. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time

before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's type of device, operating system, storage capacity, and computer habits.

7. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting the Internet activities such as whether a computer contains specific applications or software, when the computer was sharing files and some of the files which were uploaded or downloaded, as well as the date, time, means, and individual with which the user of the computer was contacting via electronic communication. Such information is often maintained indefinitely until overwritten by other data.

8. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

9. Your Affiant believes there is probable cause to believe that things that were once stored on the “**SUBJECT ITEM**” may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

10. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the “**SUBJECT ITEM**” because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the electronic device and the application of knowledge about how an electronic device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how an electronic device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to receive, store or send child pornography, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device

used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

Summary of the Investigation to Date

11. Beginning in September 2019, the HSI Internet Crimes Against Children (ICAC) Task Force and Arkansas State Police with assistance from local law enforcement agencies, set up an operation to target online predators during the 2019 Bikes, Blues and BBQ Rally in Northwest Arkansas. As a part of the operation, undercover law enforcement agents put out multiple advertisements on online websites and mobile applications or “apps.” On or about September 23, 2019, GATEWOOD responded to an undercover Plenty Of Fish posting where an Arkansas undercover law enforcement officer was representing themselves as a mother. Between September 23 and September 24, 2019, GATEWOOD, utilizing the accounts “gearz007” and “mbrown988” and representing himself as “Aaron” engaged in messages with the believed mother of the minor female. GATEWOOD and the undercover agent then exchanged cellular phone numbers and continued their conversation via text message. GATEWOOD communicated with the undercover agent utilizing the phone number 479-502-XXXX. During these text conversations, GATEWOOD made multiple statements regarding what he wanted to do to the believed 6-year-old child when he met the believed mother. In particular, GATEWOOD stated “her sit on my face while you suck on my cock.”

12. On September 24, 2019, GATEWOOD made arrangements with the undercover agent acting as the mother to meet to hang out with her and her daughters, including the 6 year old. The undercover agent suggested GATEWOOD bring lubricant for the 6 year old. On September 24, 2019, GATEWOOD was encountered as he arrived at the prearranged meeting

location discussed with the believed mother of the six (6) year old minor female for the sexual encounter. At the time of his arrest for violations of Arkansas state laws, GATEWOOD was found to be in possession of a Samsung Galaxy S7 bearing SN R58H817K83P (“**SUBJECT ITEM**”).

13. Following his encounter and subsequent arrest, GATEWOOD was transported to the HSI Fayetteville, Arkansas Field Office and escorted into an interview room. GATEWOOD told your Affiant the Samsung he was arrested with was the only device he used to communicate with the undercover agent. GATEWOOD stated that he did not have the Plenty of Fish application but accessed the site directly from the Internet. The “**SUBJECT ITEM**”, which was the only electronic device located on GATEWOOD at the time of his arrest, is believed to be the electronic device utilized to communicate with the undercover agent through his personal POF account and phone number.

14. On November 12, 2019, a search warrant (5:19CM123) for the “**SUBJECT ITEM**” was obtained in order to locate evidence of Attempted Online Enticement of a Minor in violation of Title 18, United States Code Section 2422(b). On November 15, 2019, while conducting this search, it was revealed the “**SUBJECT ITEM**” contained evidence of child pornography. Specifically, the search yielded the following:

Filename: 20190530_011253.mp4
File path: Media/Phone/DCIM/Camera/20190530_011253.mp4
Creation date: 5/30/2019 1:20:37 AM
MD5: 2ae32a4c0a7d4533fdb1c6eaf0589857

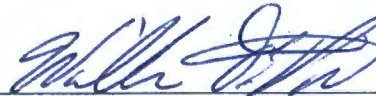
This video is approximately 07:41 (mm:ss) in length and depicts a prepubescent white female lying on a bed. The sheets are an off-white color with arrows printed on them. The child is partially covered with a camouflage colored blanket and is wearing white cotton style panties, with black pants or shorts. An unidentified white male is observed pulling the child’s panties aside and exposing her vagina to the camera. At approximately 04:09 (mm:ss) in the video, the male exposes his erect penis to the camera and appeared to be masturbating. At approximately 04:35 (mm:ss) the male rubs his exposed penis on the child’s buttocks and vaginal area. At approximately 05:35 (mm:ss) the male digitally penetrates the child’s vagina. At approximately 07:07 the male puts his

face between the girl's legs and appears to be performing oral sex on her. While performing oral sex on the child, the males head is exposed to the camera and his hair is described as long (shoulder length) and shaggy.

15. The search was then suspended pending an additional search warrant that includes authorization to search for child pornography.

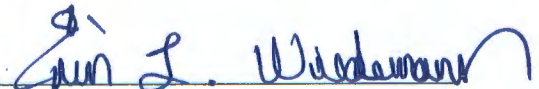
Conclusion

16. Based on the foregoing information, probable cause exists to believe there is located on a Samsung Galaxy S7 bearing identification number R58H817K83P, the "SUBJECT ITEM", evidence of violations of Title 18, United States Code, Sections 2251(a), 2252 and 2522A. Your Affiant prays upon his honorable court to issue a search warrant for the "SUBJECT ITEM" for the item set forth in attachment "B" (which is attached hereto and incorporated herein by reference), that constitute evidence, fruits, and instrumentalities of violation of Title 18, United States Code, Sections 2251, 2252 and 2522A.



William DeVito, Special Agent
Homeland Security Investigations

Affidavit subscribed and sworn to before me this 20th day of November 2019



Erin L. Wiedemann
United States Magistrate Judge